AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, William C. Nixon, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant to search the premises at 267 Permission Road, Raymore, Missouri 64083, the current residence of BRIAUNA ADMAS, further described in Attachment A, for the items in Attachments B. The subject premises are located in the Western District of Missouri.

2. I am a Special Agent with the Internal Revenue Service – Criminal Investigation (IRS-CI) and have been employed in this capacity since July 2022. I am currently assigned to the St. Louis Field Office and primarily conduct tax related investigations. My duties and responsibilities as a Special Agent include conducting criminal investigations of alleged criminal violations found in Title 18, Title 26, and Title 31 of the United States Code.

3. During my assignment as a Special Agent with IRS-CI, I completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center and the Special Agent Basic Training program conducted by the IRS's National Criminal Investigator Training Academy. I have received extensive training in, and have participated in, a variety of complex financial investigations including tax fraud and money laundering. I have also received extensive training in, and conducted, search and seizure warrants. In addition to my training and experience, I hold Bachelor of Science degree from Missouri State University in Accounting and Bachelor of Science degree from the University of Arkansas in Economics.

4. Based on my training, experience and participation in other investigations involving financial and tax related crimes, I know that:

a. Individuals committing financial or tax related crimes often place proceeds of a crime in names other than their own to avoid detection by law enforcement agencies;

b. When individuals place proceeds of a financial or tax related crime in a nominee name, they often utilize their own address or the address of an associate to perpetrate the financial or tax related crime;

c. Even though the proceeds of a financial or tax related crime may be placed in another person's name or business's names, the individual committing the financial or tax related crime continues to use the proceeds and exercise dominion and control over them;

d. Because individuals committing financial or tax related crimes continue to use and maintain control over the proceeds, they also maintain documents relating to their use and control of these proceeds. These documents include tax related documents and financial statements.

e. Where individuals committing financial or tax related crimes amass large cash proceeds from financial or tax related crimes, the individuals attempt to legitimatize the proceeds. To accomplish these goals, individuals committing financial, or tax related crimes utilize domestic banks, securities, cashier's checks, money drafts, pre-paid debit cards, stored value cards, real estate, business fronts and tax related documents;

f. All individuals, whether their income is from legal, legitimate sources or from illegal sources, such as financial or tax related crimes, commonly keep in their homes documents pertaining to their obtaining, transferring, investment, and/or expenditure of proceeds, such as: currency, financial instruments, precious metals and gemstones, jewelry, books, records, invoices, receipts, records of real estate transactions, bank

statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashiers' checks, bank checks, safe deposit keys, tax related documents, and business records. These items are maintained by individuals committing financial crimes and tax related crimes within their residences, vehicles, businesses, or other locations over which they maintain dominion and control;

g. Individuals committing financial or tax related crimes often utilize electronic equipment such as computers, cellular telephones, facsimile machines, and telephones to generate, transfer, record and/or store the information described above;

h. Individuals committing financial or tax related crimes maintain addresses, telephone numbers, and messages in books, papers and/or cellular telephones, of their associates;

5. The information in this affidavit is based on information provided to me by other law enforcement officers and other persons described in this affidavit. While preparing this affidavit and conducting the present investigation, I have consulted with and read the reports of the agents whose actions are documented in this affidavit. The information in this affidavit is submitted for the limited purpose of establishing probable cause in connection with the present applications and is not intended as a complete statement of all facts related to this investigation. The information provided is based on my personal knowledge and observation during this investigation, information conveyed to me by other law enforcement officials, and my review of records, documents, and other evidence obtained during the investigation.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A),

& (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. The United States, including the IRS-Criminal Investigation (IRS-CI) and the Kansas City, Missouri Police Department (KCPD), are conducting an investigation of BRIAUNA ADAMS, regarding violations of violations of Title 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1349 (wire fraud conspiracy) 18 U.S.C. § 1956(a)(1)(B)(i) (money laundering-concealment), and 18 U.S.C. § 1028(A) (aggravated identity theft).

8. The IRS-CI and KCPD are investigating a fraudulent PPP loan scheme in which BRIAUNA ADAMS is identified as being a promotor of a fraudulent PPP loan scheme and a benefactor of the illegal proceeds. ADAMS is believed to have submitted fraudulent documents to obtain a PPP loan in her own name and also fraudulent documents in the names of others, to include the names of stolen identities, in order to obtain the PPP loan funds. ADAMS is believed to have also opened bank accounts in the names of those individuals where the proceeds of the fraudulent PPP loans were deposited and transferred to accounts controlled by ADAMS. During this investigation, it was discovered that ADAMS unlawfully obtained multiple United States Treasury checks, payable to other individuals, and deposited the stolen checks or altered them in order to deposit the checks in ADAMS' own account, into an account controlled by ADAMS or into the account of an accomplice before transferring the illicit funds into her own accounts. ADAMS created her own fraudulent driver's licenses in the names of stolen identities to obtain

high end apartments, utilities, and bank accounts to cash some of the fraudulent United States Treasury checks. ADAMS' involvement in the fraudulent United States Treasury check scheme was found to have a potential fraud-related financial loss of over $1,988,551.00.

The CARES Act

9. The U.S. Small Business Administration (SBA) is an executive branch agency of the United States that provides support to entrepreneurs and small businesses. The mission of the SBA is to maintain and strengthen the nation's economy by enabling the establishment and viability of small businesses and by assisting in the economic recovery of communities after disasters. Under the provisions of The CARES Act, $2.2 trillion dollars in economic stimulus was passed by the 116th U.S. Congress and signed into law by President Donald Trump in March 2020, in response to the economic decline caused by the COVID-19 pandemic in the United States.

Paycheck Protection Program Loans

10. The CARES Act allowed for the authorization of up to $349 billion in forgivable loans to small businesses for job retention and certain other expenses, through the Paycheck Protection Program (PPP). These loans had government backed guarantees. In or around April 2020, Congress authorized over $300 billion in additional PPP funding.

11. To obtain a PPP loan, a qualifying business was required to submit a PPP loan application, signed by an authorized representative of the business, to a lender that was participating in PPP. The PPP loan application required the business (through its authorized representative) to acknowledge the program rules and make certain affirmative certifications in order to be eligible to obtain the PPP loan. One affirmative certification required the business to certify that it was in operation on February 15, 2020, and had employees for whom it paid salaries. Further, in the PPP loan application, the applicant (through its authorized representative)

was required to state, among other things, the business's average monthly payroll expenses and the number of employees. These figures were used to calculate the amount of money the small business was eligible to receive under the PPP. In addition, the applicant was required to provide documentation showing its payroll expenses.

12. A business's PPP loan application was received and processed, in the first instance, by a participating lender. If a PPP loan application was approved, the participating lender funded the PPP loan using its own monies, which are guaranteed by the SBA. Data from the application, including information about the borrower, the total amount of the loan, and the listed number of employees, was transmitted by the lender to the SBA in the course of processing the loan.

13. PPP loan proceeds were required to be used by the business on certain permissible expenses: payroll costs, interest on mortgages, rent, and utilities. The PPP allowed the interest and principal on the PPP loan to be entirely forgiven if the business spent the loan proceeds on these expense items within a designated period of time after receiving the proceeds and used a certain amount of the PPP loan proceeds on payroll expenses.

PPP Loans

BRIAUNA ADAMS

14. A review of PPP loan records from Kabbage (Kabbage is a portal for PPP loans) for BRIAUNA ADAMS revealed the following records were provided during her application process:

a) A Borrower Application Form dated August 4, 2020, ADAMS reported her average monthly payroll to be $7,800.

b) A 2019 US Individual Tax Return Form 1040 Schedule C in which ADAMS reported to be a sole proprietor as an "independent contractor" with a total 2019 gross earnings of only $8,500.

c) A Wells Fargo bank statement in the name of BRIAUNA ADAMS for an account ending in #2858, dated February 26, 2020, showing her address at 12005 Smalley Ave, Grandview, MO.

d) On August 4, 2020, the Kabbage PPP loan, in the amount of $19,499 was deposited into the Wells Fargo account ending in #2858.

15. According to ADAMS' credit history report from Early Warning Services, the Wells Fargo account was opened in January of 2020. The account status on August 7, 2020, shows it was overdrawn and closed on August 10, 2020, just three days after receiving the PPP loan funds, indicating the PPP loan funds were quickly transferred out of this account as well.

16. Tax records filed by ADAMS with the IRS show she reported income for 2019 of $1 and did not report any Schedule C income. The records from the IRS also show ADAMS' earned wages in 2019 from various employers totaling $12,647, even though this income was not reported on her tax return. The IRS records did not show any Form 1099 for contract income. Your affiant believes the tax return submitted to Kabbage was not a true tax return, rather fraudulent documents to make Kabbage believe she had the income stated on the loan application. ADAMS did not file a 2020 tax return according to records obtained from the Internal Revenue Service.

17. On April 3, 2023, a review of records from Navy Federal Credit Union for accounts belonging to BRIAUNA ADAMS revealed the following.

a) ADAMS was confirmed to be the sole owner of checking account ending in #1063. When the account was opened, ADAMS provided her home address of 12005 Smalley Ave, Grandview, MO.

b) ADAMS owns account ending in 6365 jointly with Bridget Gonzales. An address in Dallas, TX was provided to Navy Federal Credit Union for Gonzales' home address, however, the statement address is 12005 Smalley Ave., Grandview, MO 64030, ADAMS' residence.

c) The joint account with Gonzales was used to transfer PPP loan proceeds between other "borrowers" and ADAMS.

d) Reviewing the monthly bank statements for account ending in #1063, ADAMS was the recipient of numerous large transfers from multiple Navy Federal Credit Union accounts in the names of Pariss Nunez, Chastity Moore, London Atil, Lamonte Burge and Lashonda Fuller. A check of the free public resource website, https://www.federalpay.org/paycheck-protection-program, revealed all of the listed individuals received a PPP loan in their name, except Pariss Nunez. According to IRS records, Nunez' loan application was approved through Itria Ventures LLC but the last known status states it was cancelled.

Ciarra Henderson

18. A review of records from Itria Ventures LLC for Ciarra Henderson revealed the following records were provided during her application process:

a) A Borrower Application Form was submitted on February 2, 2021.

b) A Navy Federal Credit Union bank statement for checking account #3733 and savings account #1643 dated January 10, 2020, to February 9, 2020.

c) A 2019 US Individual Tax Return Form 1040 Schedule C in which Henderson reported to be the sole proprietor of a "children's and infants clothing store" business with 2019 gross earnings of $144,080.

d) IRS records revealed Henderson did not file taxes in 2019 and her reported gross income for 2018 was only $4,405.

e) An Authorization for PPP Loan Disbursement and ACH Debit form was completed for closing on February 21, 2021, which provided a different account number at Navy Federal Credit Union ending in #9085.

f) On March 3, 2021, the Itria Ventures PPP loan, in the amount of $20,832.50 was deposited into the Navy Federal Credit Union account ending in #9085.

19. On April 3, 2023, records were obtained from Navy Federal Credit Union for all accounts associated to Ciarra Henderson, including the accounts. A review of the records revealed the following:

a) Savings account ending in #1643 does not belong to Ciarra Henderson.

b) Checking account ending in #3733 is in the name of Ciarra Henderson but it was not opened until February 16, 2021. The statement provided to Itria Ventures LLC was dated *January 10, 2020 through February 9, 2020*, these dates were *before* the account was opened. Additionally, Itria Ventures LLC records show their application was digitally signed on February 13, 2021, three days *before* this account was opened at Navy Federal Credit Union.

c) Checking account #9085 was opened at the same time as the checking account ending in #3733 in the name of Ciarra Henderson. The address used to open both accounts was 12005 Smalley Ave, Grandview, MO.

d) The accounts opening deposit were funded from ADAMS' Navy Federal Credit Union account.

e) Under the membership eligibility section, the sponsoring Navy Federal Credit Union member's name was listed as Daisha Sanders, who was indicted for wire fraud and money laundering relating to fraudulent PPP loans (4:24-cr-00029-BP).

f) According to the bank statements, the $20,832.50 PPP loan was deposited into Henderson's account on March 3, 2021, the funds were immediately depleted by March 5, 2021. These funds were transferred and laundered from the Henderson account, through the Gonzales account, and ultimately controlled and deposited into ADAMS' account.

20. On September 13, 2023, Henderson was interviewed regarding her PPP loan. Henderson advised she had never applied for a PPP loan, never gave anyone permission to apply for one on her behalf and did NOT receive any funds from a PPP loan. Henderson also stated she had no idea an account was opened at Navy Federal Credit Union in her name and had no knowledge of who opened the account. Henderson stated her identity was stolen by BRIAUNA ADAMS and believed it was after she lost her purse in October 2020. Henderson advised her driver's license was in the purse when she lost it, however she was unable to explain how her Wells Fargo bank statement and replacement driver's license were used to apply for the PPP loan. Henderson stated she and ADAMS have a mutual friend who had informed Henderson that ADAMS was responsible for it and showed her ADAMS' social media accounts where she often makes "posts" about her fraudulent activities. Henderson, with the help of her mutual friends, was able to find ADAMS' accounts on Instagram, X, Facebook and TikTok and provided screenshots of ADAMS' posts to investigators.

21. Henderson stated she has never opened or owned an account at Navy Federal Credit Union and never gave anyone permission to do it on her behalf. Henderson stated she had no idea who Bridget Gonzales or BRIAUNA ADAMS are and never sent them any money.

22. A review was conducted of the screenshots provided by Henderson of ADAMS' social media accounts which revealed they contained numerous photographs of a female who appears to be ADAMS with large sums of cash, numerous cell phones, SIM cards for cell phones, a Maryland ID with the photograph and name covered up and at least one photograph of a partially covered Navy Federal Credit Union bank statement bearing the name BRIAUNA L. ADAMS with a zip code of 64030 visible. The following social media accounts and information was observed:

a) X, formerly Twitter, account identified as "the motion @bremoneyy365" with the following posts:

i. 10-04-20, "you ain't no scammer if you only bussing one state with 3 profiles gtf off my line tf". See EXHIBIT 1

ii. 02-04-21, "I'm a be plain honest mfs be saying they scammers but don't be changing the IP address don't use socks don't know what a rdp is for they computer. Don't clear they cookies don't have a bitcleaner nun and want me to hold they hand all the way. Nooo don't know shit.:" See EXHIBIT 2

iii. 02-07-21, " scammers over trappers." *See* EXHIBIT 2

iv. 05-15-22, "I kno a scammer that will leak yo addy" See EXHIBIT 2

v. There is an undated tweet that contains photos of stacks of U.S. currency. *See* EXHIBIT 3

b) Instagram/Facebook display name only containing an emoji of a bag of money:

i. 12-12-21, photograph of what appears to be U.S. currency, individually bundled, with a caption of "50k type of day." *See* EXHIBIT 4

c) An unknown social media account for "Bremoney365", that contained a screenshot of a TikTok account with a display name of "@breallvre" in the lower right corner. The undated screenshot depicted ten cell phones and a large amount of what appears to be US Currency in $100 and $20 bills spread out. *See* EXHIBIT 5

d) Instagram/Facebook display name of "BIG BRE FLEX" contained the following:

i. 03-24-21, photograph of a set of keys and several cell phones sitting on the center console of a vehicle with a caption of "9 phones that's why I don't answer." *See* EXHIBIT 6

ii. 05-28-21, photograph of ADAMS with a large stack of what is believed to be U.S. currency. *See* EXHIBIT 7

iii. 06-27-21, photograph of two cell phones with the screens showing CashApp direct deposit notifications for what appears to be in the amount of $9,875. *See* EXHIBIT 8

23. Bremoney365 is the current Instagram username that can be located for ADAMS from the search bar. The posts are currently private.

24. The following chart shows a few of the loans that have been identified as fraudulent by reviewing the loan records and observed payments between the borrower and ADAMS.

Name	**Loan Amount & Application Date**
Adams, Briauna	$19,499 8-4-2020
Gonzales, Bridget	$20,833 4-10-2021
Henderson, Ciarra	$20,832.50 2-21-2021
Moore, Chastity A	$20,832.50 2-10-2021
Atil, London O. Two Loans	1) $20,832.50 2-7-2021 2) $20,832 4-5-2021
Fuller, Lashonda C.	$20,832 4-8-2021 All loan proceeds went to ADAMS
Jones, Kourtney A. Two Loans	1) $20,832 2-27-2021 2) $20,833 3-23-2021 & 4-23-2021
Ridge, Sasha S.	$20,832 3-22-2021 or 3-29-2021
Hibbs, Carla C.	$20,832 4-7-2021

February 2024 Search Warrant

25. There are several other additional loans that are still being reviewed by agents. These loans were identified through a February 2024 search warrant (Case No. 24-SW-00013-JAM) on ADAMS' gmail account, briaunaadams@gmail.com. While reviewing the records from the search warrant, a significant number of emails were sent from briaunaadams@gmail.com to an email called scamjesuss@outlook.com. Those emails contained attachments that included IRS Form Schedule C, Forms 1099-Misc, bank statements, and pictures of driver's licenses. The subscriber records show scamjesuss@outlook.com was set up as an email account by ADAMS on March 2, 2021.

26. The analysis of the briaunaadams@gmail.com search warrant showed approximately 129 @yahoo.com email addresses that sent an email to the briaunaadams@gmail.com account with the subject "yo," which are then forwarded from ADAMS

to scamjesuss@outlook.com. Subsequent emails contain attachments that are the documents believed to be false documents used to obtain PPP loans.

27. The following is a sample of the individuals with addresses in the Western District of Missouri:

Borrower	Tax Gross Income	Bank Statement	Loan Date	Loan Amount	Status
VaRhonda Burnett	$ 147,412.00	Arvest	3/23/2021	$ 20,832.00	Paid/Forgiven
Shyaine Hughes	$ 147,412.00	Arvest	5/11/2021	$ 20,832.00	Delinquent Disbursed
Trisha Hughes	$ 147,412.00	Arvest	4/5/2021	$ 20,832.00	Paid in Full
Shalonda Farmer	$ 147,412.00	Arvest	3/30/2021	$ 20,832.00	Paid in Full
Kanesha Williams	$ 153,636.00	Arvest	3/23/2021	$ 20,832.00	Delinquent Disbursed
Jarai Porter	$ 153,636.00	Arvest	4/3/2021	$ 20,832.00	Paid/Forgiven
Amya Tabron	$ 147,412.00	Wells Fargo	4/3/2021	$ 20,832.00	Delinquent Disbursed
Rickeish Parish	$ 147,412.00	Wells Fargo	4/5/2021	$ 20,832.00	Paid/Forgiven
Taisha Lane	$ 147,412.00	Wells Fargo	3/24/2021	$ 20,832.00	Paid/Forgiven
Timika Evans	$ 153,636.00	Wells Fargo	3/22/2021	$ 20,832.00	Paid/Forgiven
Marteono Gonzales	$ 153,636.00	Wells Fargo	4/3/2021	$ 20,832.00	Delinquent Disbursed
LeTonja Saulsberry	$ 153,636.00	Wells Fargo	3/11/2021	$ 20,832.00	Paid/Forgiven

28. In the emails, each of the bank statements for Arvest contained the same transactional data (balances, account activity), only the name and account number changed. The same is true for Wells Fargo statements. The Arvest Bank statements all had a statement date ending February 13, 2020.

29. The search warrant records analyzed for the above individuals also contains two different IRS Form Schedule C. One set of the Schedule Cs contain the gross income figure $147,412 and identical expenses, and the second set of Schedule Cs contain the gross income figure $153,636 and identical expenses.

US TREASURY CHECKS

30. On March 12, 2024, an account was opened at Academy Bank, in Fairway, Kansas by an unknown white female who was later determined to be using the stolen identity of Leslie Lawson. Academy Bank is a financial institution, as that term is defined in Title 18, United States Code, Section 20, in Missouri and other states. Approximately two hours after the account was opened, a stolen U.S. Treasury check in the amount of $10,590.05 was deposited at the Academy Bank ATM in Gladstone, Missouri by a black female. Surveillance photos from the ATM show ADAMS as the person depositing the stolen treasury check in the name of Leslie Lawson.

31. The bank flagged the check as suspicious and did not credit the account. The real Leslie Lawson was interviewed and stated she was a resident of Louisiana. Lawson had been expecting a check from the Internal Revenue Service and had been a recent victim of identity theft.

32. On May 6, 2024, the United States Treasury check was examined by the Forensic and Digital Science Laboratory of the Treasury Inspector General for the Tax Administration who deemed the check genuine. On May 8, 2024, latent prints were identified on the check as fingerprints belonging to ADAMS.

33. On June 18, 2024, ADAMS presented a fraudulent US Treasury check in the amount of $450,504.66 for deposit into her individual account ending in #0663 at Fidelity Investments. The copy of the US Treasury check provided by Fidelity showed it was made out to ADAMS at 12005 Smalley Avenue, Grandview, Missouri 64030, and dated May 10, 2024.

34. Records from the Burueau of Fiscal Services show the original check in the amount of $450,504.66 was payable to PTC C/F IRA FBO M*** C T***** with the originating agency the Thrift Savings Plan.

35. According to records from Fidelity Investments, ADAMS opened her first account in May 2024 from an IP address of 136.34.44.44. ADAMS provided a mobile number of 816-530-1044 and a daytime phone number of 816-530-1115. ADAMS opened additional accounts and ordered cards for the accounts online on June 14, 2024, from the same IP address of 136.34.44.44.

36. ADAMS utilized multiple bank accounts to conceal the source and location of the proceeds from the $450,504.66 check she deposited as part of her wire fraud scheme, once those accounts were opened, transfers were conducted to move the money from the original bank of deposit to two other bank accounts, where she then attempted utilize the proceeds.

37. On April 10, 2024, ADAMS opened an account a Central Trust Bank, using her MO non-driver's license and the address of her mother. ADAMS could not use her real address, 1125 Grand Blvd., Apt. 0411, in downtown Kansas City, because that property was rented in the name Valeria Cerrillo. ADAMS used a false ID with Cerrillo's name on it to rent the apartment.

38. On May 28, 2024, ADAMS opened an account at Fidelity Investments, again using her mother's Grandview, MO address.

39. On June 14, 2023, ADAMS opened Truist Bank account ending in 8147 using her MO non-driver's license but provided a home address of 2801 Crestbrook Lane, Grand Prairie, TX. ADAMS was living in Kansas City.

40. On June 18, 2024, ADAMS deposited the altered check in the amount of $450,504.66 into the Fidelity account.

41. On June 27, 2024, ADAMS electronically transferred $8,000 to Central Trust Bank with the intent to conceal or disguise the source and location of the proceeds.

42. On June 27, 2024, ADAMS electronically transferred $4,000 to Truist Bank with the intent to conceal or disguise the source and location of the proceeds.

43. Hours after the transfers, Fidelity Investments received notification the U.S. Treasury check was fraudulent. The bank reversed the deposit leaving the account with a negative balance, causing Fidelity Investments to suffer a financial loss of $11,994.96.

44. Regarding the $4,000 transferred by ADAMS to Truist Bank account ending in #8147, ADAMS opened her Truist Bank account on April 10, 2024, online from a T-Mobile device and provided a T-Mobile phone number of 816-530-1044. The account wasn't accessed again until April 27, 2024 when it was done from the same Google IP address of 136.34.44.44. The $4,000 transfer was done on June 27, 2024, and ADAMS immediately forwarded $2,500 of it in two Zelle payments to a Kyerra Wilson and $1,500 in a Zelle payment to "Honey".

45. Regarding the $8,000 transferred by ADAMS to the Central Trust Bank account ending in #2214, bank records showed ADAMS opened the account on April 10, 2024, online from the Google IP address of 136.34.44.44. The $8,000 transfer was done on June 27, 2024, and the next day ADAMS conducted a $2,000 cash withdrawal in Riverside, Missouri and made a $683 Evergy utility payment for an account in Kansas City, Missouri. A review of the remaining transactions revealed between July 1, 2024, and July 3, 2024, there were numerous large payments to Sway Properties, a property management company.

46. On September 23, 2024, records were received from T-Mobile that confirmed the phone number of 816-530-1115, used by ADAMS on the Fidelity Investments accounts was registered to ADAMS and service began on May 31, 2024.

47. On September 30, 2024, Google Fiber records were obtained for IP address 136.34.44.44, showing it was registered at 1125 Grand Boulevard, Apt. 411, Kansas City, Missouri 64106, under the name of Valeria Cerrillo with a phone number of 816-530-1044. The phone number associated to the Google Fiber account was one of the numbers used by ADAMS to register for the Fidelity Investments bank account. A computer check of the Cerrillo name revealed the individual is a Hispanic female who resides in the Richmond, Texas area.

48. On September 30, 2024, investigators interviewed the complex managers at The Grand Apartments at 1125 Grand Boulevard, Kansas City, Missouri. Management staff confirmed the name of the tenant in penthouse apartment #411 was Valeria Cerrillo, however she vacated the apartment on July 15, 2024 after non-payment of rent. The Texas driver's license photo belonging to Valeria Cerrillo was presented to management at which time she stated it was NOT the Valeria Cerrillo who lived at The Grand Apartments. The Missouri driver's license photograph of ADAMS was presented, before anything was said, management immediately confirmed ADAMS to be the female renter she knew to be Valeria Cerrillo. Management provided a copy of the driver's license used to rent the apartment, which was a Texas driver's license in the name of Cerrillo, but contained a black and white photograph of ADAMS.

49. Management advised they entered the apartment on July 30, 2024 and confirmed the apartment had been abandoned. ADAMS had moved out but left behind several high-end electronics and other personal items. Management found at least two Florida driver's licenses, other Texas driver's licenses and social security cards in other names that were turned into police. According to The Grand Apartments, they suffered a financial loss in back rent totaling $14,185.20.

50. A check of police records revealed the identifications from ADAMS' apartment at The Grand were recovered as safekeeping under KCPD CRN #24-059582 and destroyed according to department policy on September 23, 2024. There were two Florida driver's licenses in the names of Hollis P. Nelson II and Charles F. Delavergne as well as a Georgia driver's license in the name of Tammy C. Garrison. Due to the property having been destroyed, investigators viewed the bodycam footage from the officer who recovered the property. The photograph on the Georgia driver's license in the name of Tammy Garrison was immediately recognized as being the same white female who opened the account at Academy Bank using the stolen identity in the name of Leslie Lawson and where ADAMS deposited the stolen $10,590.05 US Treasury check.

51. The real Valeria Cerrillo of Richmond, Texas, was contacted and interviewed over the phone. Cerrillo had no idea her identity was being used. She confirmed her current residence in Texas and advised she has no ties to the Kansas City, Missouri area. Cerrillo advised she does not know ADAMS and did not give her permission to use her name and personal information to rent an apartment, obtain utilities or any other line of credit.

52. On August 15, 2024, ADAMS presented a fraudulent US Treasury check worth $1,445,443.69 for deposit into her individual account ending in #9602 at Charles Schwab and Co. The copy of the US Treasury check showed it to be made out to ADAMS at 12005 Smalley Avenue, Grandview, Missouri 64030 and dated June 25, 2024. ADAMS opened the Schwab account on July 27, 2024, from Comcast Cable IP address of 73.185.255.206. Between August 15, 2024, and August 16, 2024, after the check was deposited, ADAMS accessed the account nine times from a Comcast Cable IP address of 24.2.15.231.

53. On October 7, 2024, Comcast Cable records were obtained for the IP addresses of 73.185.255.206 and 24.2.15.231 revealing both were located at 267 Persimmon Rd, Raymore,

Missouri, in the name of Myranda Baumgartner with the phone number of 816-530-1115. The phone number of 816-530-1115 was immediately recognized as being the T-Mobile phone number registered to ADAMS. A computer check of the Myranda Baumgartner name revealed her to be a white female who lives in Athens, TX.

54. On October 8, 2024, investigators responded to the 267 Persimmon Rd, Raymore, Missouri address and observed it to be a brand-new townhouse within the Oak Ridge Falls subdivision. The property management company was identified as Sway Properties, the same company ADAMS made payments to in July 2024 using the illicit funds from the fraudulent US Treasury check at Fidelity Investments. Contact was made with the property manager who confirmed "Myranda Baumgartner" was still residing at the address and moved in July of 2024. The property manager provided a photograph of the driver's license presented to their leasing office to rent the unit. It was a Texas driver's license with the name Myranda Elise Baumgartner of Athens, Texas, but with the same black and white photograph of ADAMS that was used on the Valeria Cerrillo Texas driver's license.

55. On October 8, 2024, contact was made with the real Myranda Baumgartner in Athens, Texas. Baumgartner advised she is a permanent resident of Athens, Texas and has no ties to the Kansas City, Missouri area. She was not aware of anyone renting an apartment in her name and never gave anyone permission to do so. Baumgartner advised no one had permission to obtain any line of credit or utility service in her name.

56. On October 8, 2024, additional records were received from T-Mobile confirming ADAMS to be registered to both phone numbers of 816-530-1044 AND 816-530-1115. T-Mobile also provided payment history for both of ADAMS' phone numbers. Among the payment sources were three not in the name of ADAMS. There were two VISA cards in the name of Valeria Cerrillo and a VISA card ending in #7192 in the name of Sharyl Durham. Valeria Cerrillo was the identity theft victim of the lease at The Grand Apartments where ADAMS was residing up until July of 2024. The VISA card #7192 matches the last four numbers of the credit card currently being used to pay rent at the townhouse at 267 Persimmon Rd, Raymore, Missouri in the name of identity theft victim, Myranda Baumgartner.

57. During the course of the investigation into ADAMS' identity theft activities, a police records check revealed in 2022, ADAMS was involved in an altercation with a Shawntae McGuire in Kansas City, Missouri that led McGuire to flee to Frisco, Texas for her safety. Once in Frisco, Texas, McGuire filed a police report, Frisco PD #22-017304, stating she had been ADAMS' business partner prior to the altercation. McGuire collected several fraudulent identities, credit and debit cards and documents from ADAMS' residence and turned them into the police. Copies of these identities were reviewed by investigators at which time it was noted at least 24 contained the same photograph of ADAMS with various names. This

photograph was the same one from the Texas driver's licenses in the names of Cerrillo and Baumgartner in this investigation, See EXHIBIT 9.

59. On November 7, 2024, contact was made with the property manager at Sway Properties who advised according to their records ADAMS is still residing at the residence.

60. On November 12, 2024, at 7:59 p.m., a person who appeared to be ADAMS was observed through a covert camera entering the garage of the SUBJECT PREMISES.

61. Based on the above-mentioned financial records, conversations, and observations by investigators, it is believed the SUBJECT PREMISES is ADAMS' residence, and that the SUBJECT PREMISES is where ADAMS maintains her personal belongings, financial records, identifications and other pertinent documentation.

62. Investigators believe ADAMS committed one or more of the Target Offenses. Considering the last time ADAMS left an apartment at The Grand she left behind several different fraudulent driver's licenses, investigators believe she is still in possession of many more to maintain her current lifestyle. Investigators also believe that the remaining proceeds of the fraudulent checks (in United States currency) and other evidentiary documentation of the Target Offenses will be located at the SUBJECT PREMISES.

63. Through my training and experience I know that individuals who commit financial fraud often hold onto documents such as financial records, correspondence, and personal records that relate to their financial activities for long periods of time. I also know through my training and experience that individuals keep these documents at their primary/permanent residence.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

64. Based upon the information set forth above and immediately below, I believe there is probable cause to conclude that within each of the Subject Premises there is evidence and

instrumentalities of the Subject Offenses. Accordingly, I request that the Court issue a search warrant for each of the Subject Premises, and the DEVICES as described, in this affidavit, and in Attachment B, for the items set forth in Attachment B to this affidavit.

65. Based on the information set forth above, my training and experience, and the training and experience of other law enforcement officers involved in this investigation, I know that it is common for persons engaged in fraud and other illegal activity, including Payroll Protection Program fraud and stolen/altered check fraud, to keep records relating to the following:

a. Records (in either electronic or paper form) relating false identifications, false tax returns, and bank accounts associated with fraudulent transactions;

b. Records (in either electronic or paper form) relating to customer, vendor, employee, and contractor transactions, including, but not limited to, financial statements, correspondence, spreadsheets, email messages, records documenting the type of financing services rendered or purchased, including customer lists, transaction dates, the cost of services to be rendered, as well as invoices, letters, and contracts;

c. Records (in either electronic or paper form) relating to employees and business associates, including, but not limited to, contact books, ledgers, invoices, email communications, correspondence, payments, etc., concerning vendors, employees, and contractors with whom the Conspirators did business.

66. Based upon my training and experience, I know that it is necessary for law abiding citizens and individuals committing fraud – to maintain other books and records sufficient to conduct ordinary financial business. These records typically include (in either electronic or paper form): ledgers, journals, receipts, invoices, bank statements, income tax returns, purchase and sale records, accounts payable and receivable records, customers' files, and payroll records.

67. Based on my training and experience, I know that individuals, both law abiding and those committing fraud to keep financial records (such as daily revenues, profits, and profit sharing) in many forms, including electronically. Consequently, I believe that the documents sought by the search warrant may be stored on computers, laptops, desktops, and cellular telephones, the DEVICES, used by the subject to conduct her illegal activities. The protocol for the search of the DEVICES pursuant to this warrant is set forth below and in Attachment B.

68. Based upon my training and experience, I know that a cellular telephone is a storage device that is capable of storing and transmitting electronic versions of documents described in this affidavit that were utilized by the subject to conduct her fraud schemes detailed in the paragraphs above.

TECHNICAL TERMS

69. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

70. As described above and in Attachment B, this application seeks permission to search for records that might be found within the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

71. I submit that if a computer or storage medium is found within the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

72. Based on actual inspection of other evidence related to this investigation, I am aware that computer equipment was used to generate, store, and email documents used in the wire fraud and bank fraud schemes.

73. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies,

transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of

mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

74. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be

required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

75. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

76. I submit that this affidavit supports probable cause for a warrant to search 267 Permission Road, Raymore, Missouri 64083, described in Attachment A, the DEVICES as described in Attachment B, and seize the items described in Attachment B.

REQUEST FOR SEALING

I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

William Nixon
Special Agent, IRS-Criminal Investigation

Telephonically aat 12:43 p.m., with signatures confirmed,
Subscribed and sworn to ~~before me~~

this 14th day of November 2024.

HONORABLE JILL A. MORRIS
United States Magistrate Judge
Western District of Missouri